Encoding method for carrying out cryptographic operations.

Technical field

The invention relates to an encryption method as disclosed in the introductory part of Claim 1, wherein at least one cryptographic sub-operation is performed on digital data stored as at least one data bit word in a storage cell or a register.

State of the art

Cryptographic operations are carried out in many data processing apparatus so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or an IC card. For such cryptographic calculations it is often necessary to initialize relevant storage sections or registers of the data processing apparatus with operands. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

In order to calculate the cryptographic algorithms, logic combinations of operands or intermediate results are formed in the data processing apparatus. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This

type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus.

EP 0 482 975 B1 discloses a memory card which includes a microcircuit and at least one memory which is connected to a data processing member, the data processing member being controlled by a data signal from outside the card and delivering a command transmission signal in response to said data signal, at a given instant, said command transmission signal being delayed by a predetermined period of time (T) relative to the reception of the data signal, the period of time (T) being selected so as to be variable in time on a random basis in order to enhance the security. Crypto analysis on the basis of a current variation during the writing of the memory, however, cannot be precluded by such a system.

Implementation of the invention, object, solution, advantages

It is an object of the present invention to provide an improved method of the kind set forth which eliminates the described drawbacks and effectively prevents crypto analysis by observation of current consumption of a data processing apparatus.

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1.

To this end, in conformity with the invention a data bit word generated on the basis of random numbers is stored in a storage cell before a data bit word is written therein.

This offers the advantage that there is a non-predetermined or non-predeterminable pre-initialization which prevents information concerning the data bit word written into the memory cell from being extracted on the basis of variations of the current consumption during the writing into the storage cell. During the writing of data in such pre-initialized storage cells the current consumption changes exclusively in dependence on a difference between the Hamming weight of the written data and the unknown random number, so that this difference, and hence also the variation of the current consumption, is of a random nature and cannot be determined in advance.

There are various possibilities for the implementation of the method. According to a preferred version, the bit word based on random numbers is written into the storage cell by a processor. Alternatively, the bit word based on random numbers is written into the storage cell via a direct connection between a random number source and the storage cell.

Temporal correlation between the writing of the random number into a storage cell and the cryptographic sub-operation is avoided in that the bit word based on random numbers is stored in the storage cell at an instant in time which precedes the cryptographic sub-operation.

Brief description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. The single Figure thereof shows a flow chart concerning a preferred version of the method according to the invention.

Preferred implementation of the invention

As is shown in the sole Figure, a storage cell 10 or a register is provided for the writing and storage of data $x_i$ in the form of a data bit word via a connection 11. However, before the operand $x_i$ is written into the storage cell 10, a random number source 12 generates random numbers which are written or stored, via a direct connection 14, into the memory cell 10. In other words, the storage cell 10 is initialized by way of a random value $r_i$. Alternatively, the random value $r_i$ can also be written, via the connection 11, by a processor having previously received the random value from the random number source 12.

The instant of pre-initialization can be selected at random and preferably does not directly precede the cryptographic operation. Preferably, repeated pre-initialization of the storage section or register is performed with varying random numbers.

When the storage sections or registers thus pre-initialized are loaded with data $x_i$ in the course of a cryptographic operation, the current consumption will change exclusively in dependence on a difference between the Hamming weight of the operand $x_i$ and the Hamming weight of the unknown random number. It is impossible to extract information as regards the operands used or intermediate results on the basis of such a random difference value.

LIST OF REFERENCES

| | |
|---|---|
| 10 | storage cell/register |
| 11 | connection |
| 12 | random number source |
| 14 | connection |
| $x_i$ | data |
| $T_i$ | random value. |